



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
[www.uspto.gov](http://www.uspto.gov)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/754,813	01/04/2001	Jing Min Xu	JP919990266US1	3476
7590	12/09/2004		EXAMINER	
Ido Tuchman 69-60 108th Street Suite 503 Forest Hills, NY 11375			CHEN, CHONGSHAN	
			ART UNIT	PAPER NUMBER
			2162	

DATE MAILED: 12/09/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

<b>Office Action Summary</b>	Application No.	Applicant(s)	S J
	09/754,813	XU ET AL.	
	Examiner Chongshan Chen	Art Unit 2162	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --  
**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

#### Status

- 1) Responsive to communication(s) filed on 08 October 2004.
- 2a) This action is FINAL.                    2b) This action is non-final.
- 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

#### Disposition of Claims

- 4) Claim(s) 1-15 and 17-21 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) Claim(s) \_\_\_\_\_ is/are allowed.
- 6) Claim(s) 1-15 and 17-21 is/are rejected.
- 7) Claim(s) \_\_\_\_\_ is/are objected to.
- 8) Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

#### Application Papers

- 9) The specification is objected to by the Examiner.
- 10) The drawing(s) filed on \_\_\_\_\_ is/are: a) accepted or b) objected to by the Examiner.  
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

#### Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) All    b) Some \* c) None of:  
 1. Certified copies of the priority documents have been received.  
 2. Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.  
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

#### Attachment(s)

- |  |   |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)  | 4) <input type="checkbox"/> Interview Summary (PTO-413)                     |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)                                   | Paper No(s)/Mail Date. _____  |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)<br>Paper No(s)/Mail Date _____ | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
|  | 6) <input type="checkbox"/> Other: _____                                    |

## **DETAILED ACTION**

### ***Continued Examination Under 37 CFR 1.114***

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 8 October 2004 has been entered.
2. Claims 1-15 and 17-21 are pending.

### ***Response to Arguments***

3. Applicant's arguments, see page 6 last paragraph, filed on 8 October 2004, with respect to the rejection(s) of claim(s) 1-15 and 17-20 under 103(a) have been fully considered and are persuasive. Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection is made in view of US Patent No. 6,128,740 to Curry et al. (herein "Curry"). Curry discloses periodically retrieving CRLs (Curry, Fig. 3 & 4A, col. 3, lines 1-67). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to periodically retrieving CRLs in the system of Kocher. Because a digital certificate may have been revoked for some reason within the validity period of the digital certificate, periodically retrieving CRLs determines whether the certificate is valid and ensures the integrity of the system.

***Claim Rejections - 35 USC § 103***

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

5. This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

6. Claims 1, 4, 6-7, 10-11, 13-15 and 17-21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kocher (6,442,689) in view of Curry et al. ("Curry", 6,128,740) and further in view of Ng (6,411,956).

As per claim 1, Kocher teaches a system comprising:

a plurality of certificate authorities (CAs) in which each CA maintains and distributes digital certificates revoked by itself in the form of a certificate revocation list (CRL), and different CAs may use different CRL distribution mechanisms (Kocher, col. 2, lines 17-31, col. 3, lines 15-18);

a plurality of CRL databases for storing the consolidated CRLs from multiple CRL retrieval agents and/or the replications of CRLs, the CRL databases storing at least one individually identifiable revoked digital certificate (Kocher, col. 3, lines 15-18).

Kocher does not explicitly disclose multiple CRL retrieval agents configured to periodically retrieve CRLs at time intervals from different CAs. Curry discloses periodically retrieving CRLs (Curry, Fig. 3 & 4A, col. 3, lines 1-67). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the CRL system of Kocher by incorporating periodically retrieving CRLs in the same conventional manner as disclosed by Curry (Fig. 3 & 4A, col. 3, lines 1-67). The motivation being to determine whether the digital certificate is valid, thereby ensuring the integrity of the system.

Neither Kocher nor Curry discloses a CRL access user interface for providing a uniform set of Application Program Interfaces for users accessing the CRLs in the CRL database. Ng teaches an access user interface for providing a uniform set of APIs for users accessing the database (Ng, col. 1, lines 15-18). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the Kocher and Curry's combined system by incorporating a uniform set of APIs in the same conventional manner as disclosed by Ng (col. 1, lines 15-18). The motivation being to provide easy access to the CRLs using a single interface.

As per claim 4, Kocher, Curry and Ng teach all the claimed subject matters as discussed in claim 1, and further disclose said plurality of CRL retrieval agents include a HTTP/CRL retrieval agent, for periodically retrieving CRLs from specified HTTP servers and updating the CRL database (Kocher, col. 1, line 19 - col. 2, line 67).

As per claim 6, Kocher, Curry and Ng teach all the claimed subject matters as discussed in claim 1, and further disclose said plurality of CRL retrieval agents include a HTTP retrieval agent triggered by a HTTP request, said HTTP receiver agent verifies an authorization of the requester, if successful, said agent stores each transmitted CRL in the CRL databases (Kocher, col. 3, line 1 - col. 4, line 56, col. 10, lines 64-67).

As per claim 7, Kocher, Curry and Ng teach all the claimed subject matters as discussed in claim 1, and further disclose said plurality of CRL retrieval agents further verifies the integrity and the authenticity of the retrieved CRLs (Kocher, col. 3, line 1 - col. 4, line 56).

As per claim 10, Kocher, Curry and Ng teach all the claimed subject matters as discussed in claim 1, and further disclose said system is also adapted for consolidating and accessing at least one kind of revoked certificate list (Kocher, col. 3, line 1 - col. 4, line 56).

As per claim 11, Kocher teaches in a secure network implemented by digital certificates, a method for certificate revocation list (CRL) consolidation and access, wherein a plurality of certificate authorities (CAs) maintain and distribute the digital certificates revoked by themselves in the form of CRLs, and different CAs may use different CRL distribution mechanisms, said method comprising the steps of:

creating a plurality of CRL retrieval agents based on the CRL distribution mechanisms of CAs, for consolidating the CRLs from multiple CAs (Kocher, col. 2, line 17 - col. 3, line 18);

storing the consolidated CRLs from multiple CRL retrieval agents or the replications of CRLs into a plurality of CRL databases, the consolidated CRLs including at least one individually identifiable revoked digital certificate (Kocher, col. 2, line 17 - col. 3, line 18).

Kocher does not explicitly disclose periodically retrieve CRLs at time intervals from different CAs. Curry discloses periodically retrieving CRLs (Curry, Fig. 3 & 4A, col. 3, lines 1-67). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the CRL system of Kocher by incorporating periodically retrieving CRLs in the same conventional manner as disclosed by Curry (Fig. 3 & 4A, col. 3, lines 1-67). The motivation being to determine whether the digital certificate is valid, thereby ensuring the integrity of the system.

Neither Kocher nor Curry discloses accessing the CRLs from the CRL databases by a uniform set of Application Program Interfaces. Ng teaches an access user interface for providing a uniform set of APIs for users accessing the database (Ng, col. 1, lines 15-18). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the Kocher and Curry's combined system by incorporating a uniform set of APIs in the same conventional manner as disclosed by Ng (col. 1, lines 15-18). The motivation being to provide easy access to the CRLs using a single interface.

As per claim 13, Kocher, Curry and Ng teach all the claimed subject matters as discussed in claim 11, and further disclose said method is also adapted for consolidation and accessing all kinds of black lists (Kocher, col. 3, line 1 - col. 4, line 56).

As per claim 14, Kocher, Curry and Ng teach all the claimed subject matters as discussed in claim 11, and further disclose an article of manufacture comprising a computer usable medium having computer readable program code means embodied therein for causing certificate revocation list (CRL) consolidation and access, the computer readable program code means in

Art Unit: 2162

said article of manufacture comprising computer readable program code means for causing a computer to effect the steps of claim 11 (Kocher, col. 1, line 1 - col. 4, line 56).

As per claim 15, Kocher, Curry and Ng teach all the claimed subject matters as discussed in claim 11, and further disclose a computer program product comprising a computer usable medium having computer readable program code means embodied therein for causing certificate revocation list (CRL) consolidation and access, the computer readable program code means in said computer program product comprising computer readable program code means for causing a computer to effect the steps of claim 11 (Kocher, col. 1, line 1 - col. 4, line 56).

As per claim 17, Kocher, Curry and Ng teach all the claimed subject matters as discussed in claim 11, and further disclose a program storage device readable by machine, tangibly embodying a program of instructions executable by the machine to perform method steps for certificate revocation list (CRL) consolidation and access, said method steps comprising the steps of claim 11 (Kocher, col. 1, line 1 - col. 4, line 56).

Claim 18 is rejected on grounds corresponding to the reasons given above for claim 11.

Claim 19 is rejected on grounds corresponding to the reasons given above for claim 17.

Claim 20 is rejected on grounds corresponding to the reasons given above for claim 14.

Claim 21 is rejected on grounds corresponding to the reasons given above for claim 15.

7. Claims 2, 8 and 12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kocher (6,442,689) in view of Curry et al. ("Curry", 6,128,740) in view of Ng (6,411,956) and further in view of Ginter et al. ("Ginter", 6,658,568).

As per claim 2, Kocher, Curry and Ng teach all the claimed subject matters as discussed in claim 1, and further teach a central CRL database (Kocher, col. 2, lines 17-31, col. 3, lines 15-

Art Unit: 2162

18). Kocher does not explicitly disclose a plurality of CRL replication databases storing the replications of the CRLs of the central CRL database. Ginter discloses a plurality of CRL replication databases storing the replications of the CRLs of the central CRL database (Ginter, col. 80, line 56, col. 81, lines 19-24). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the Kocher, Curry and Ng's combined system by incorporating a plurality of CRL replication databases in the same conventional manner as disclosed by Ginter (col. 80, line 56, col. 81, lines 19-24). The motivation being to reduce the workload at the central CRL database and divide the workload among the plurality of CRL replica databases. This will improve the processing speed.

As per claim 8, Kocher, Curry and Ng teach all the claimed subject matters as discussed in claim 1, except for explicitly disclosing a particular replication architecture is used among said plurality of CRL databases in order to maintain database consistency. Ginter discloses a particular replication architecture is used among said plurality of CRL databases in order to maintain database consistency (Ginter, col. 80, line 56, col. 81, lines 19-24). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the Kocher, Curry and Ng's combined system by incorporating a replication architecture in the same conventional manner as disclosed by Ginter (col. 80, line 56, col. 81, lines 19-24). The motivation being to produce a plurality of CRL replica databases, and divide the workload among the plurality of CRL replica databases. This will improve the processing speed.

Claim 12 is rejected on grounds corresponding to the reasons given above for claim 2.

8. Claim 3 is rejected under 35 U.S.C. 103(a) as being unpatentable over Kocher (6,442,689) in view of Curry et al. ("Curry", 6,128,740) in view of Ng (6,411,956) and further in

view of Vesna Hassler (“Hassler”, “X.500 and LDAP security: a comparative overview”, Network, IEEE, Volume: 13 Issue: 6, Nov.-Dec. 1999, Page(s): 54-64).

As per claim 3, Kocher, Curry and Ng teach all the claimed subject matters as discussed in claim 1, except for explicitly disclosing said plurality of CRL retrieval agents include a LDAP/CRL retrieval agent, for periodically retrieving CRLs from specified LDAP servers and updating the CRL databases. Hassler discloses said plurality of CRL retrieval agents include a LDAP/CRL retrieval agent, for periodically retrieving CRLs from specified LDAP servers and updating the CRL databases (Hassler, page 54). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the Kocher, Curry and Ng’s combined system by incorporating a LDAP/CRL retrieval agent in the same conventional manner as disclosed by Hassler (page 54). The motivation being to provide an agent to retrieve and verify the digital certificate in LDAP system.

9. Claim 5 is rejected under 35 U.S.C. 103(a) as being unpatentable over Kocher (6,442,689) in view of Curry et al. (“Curry”, 6,128,740) in view of Ng (6,411,956) and further in view of Kaliski, B; (“Kaliski”, “Privacy Enhancement for Internet Electronic Mail: Part IV: Key Certification and Related Services”, RFC 1424, Feb. 1993, pp. 1-8).

As per claim 5, Kocher, Curry and Ng teach all the claimed subject matters as discussed in claim 1, except for explicitly disclosing said plurality of CRL retrieval agents include a RFC1424/CRL retrieval agents, for periodically sending RFC1424/CRL retrieval request and receiving CRL retrieval reply. Kaliski discloses said plurality of CRL retrieval agents include a RFC1424/CRL retrieval agents, for periodically sending RFC1424/CRL retrieval request and receiving CRL retrieval reply (Kaliski, page 1). Therefore, it would have been obvious to one of

Art Unit: 2162

ordinary skill in the art at the time the invention was made to modify the Kocher, Curry, Ng's combined system by incorporating RFC1424/CRL retrieval agent in the same conventional manner as disclosed by Kaliski (page 1). The motivation being to provide an agent to retrieve and verify the digital certificate in Internet Electronic Mail system.

10. Claim 9 is rejected under 35 U.S.C. 103(a) as being unpatentable over Kocher (6,442,689) in view of Curry et al. ("Curry", 6,128,740) in view of Ng (6,411,956) in view of Ginter et al. ("Ginter", 6,658,568) and further in view of Strellis et al. ("Strellis", 6,304,882).

As per claim 9, Kocher, Curry, Ng and Ginter teach all the claimed subject matters as discussed in claim 2, except for explicitly disclosing a hub-and-spoke replication architecture is used among said central CRL database and said plurality of CRL replication databases. Strellis discloses disclosing a hub-and-spoke replication architecture is used among said central CRL database and said plurality of CR.L replication databases (Strellis, col. 10, lines 14-21). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the Kocher, Curry, Ng and Ginter's combined system by incorporating a hub-and-spoke replication architecture in the same conventional manner as disclosed by Strellis (col. 10, lines 14-21). The motivation being to maintain the consistency between the central database and plurality of replica databases.

#### *Contact Information*

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Chongshan Chen whose telephone number is (571)272-4031. The examiner can normally be reached on Monday - Friday (8:00 am - 4:30 pm).

Art Unit: 2162

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, John E Breene can be reached on (571)272-4107. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Chongshan Chen  
December 1, 2004



JEAN M. CORRIELUS  
PRIMARY EXAMINER